

PROFINITE GROUPS WITH NONABELIAN CROWNS OF BOUNDED RANK AND THEIR PROBABILISTIC ZETA FUNCTION

Andrea Lucchini

Università di Padova, Italy

Topics in Algebra
in honour of Professor Alexandre E. Zaleskii
on the occasion of his 70th birthday
University of Milano - Bicocca 13 - 15 May 2009

Let G be a finitely generated profinite group. We consider G as a probability space (with respect to the normalized Haar measure) and denote by $P(G, k)$ the probability that k random elements generate G .

G is called **positively finitely generated** (PFG) if $P(G, k) > 0 \exists k \in \mathbb{N}$.

CONJECTURE (MANN 1996)

If G is a PFG group, then the function $P(G, k)$ can be interpolated in a natural way to an analytic function $P(G, s)$, defined for all s in some right half-plane of the complex plane.

The reciprocal of a function with these properties has some right to be called the **probabilistic zeta-function of G** . If ζ is the Riemann zeta function, then $P(\hat{\mathbb{Z}}, k) = \zeta(k)^{-1}$.

Mann proposed an approach to the problem suggested by the following results:

- $P(G, k) = \inf_{N \triangleleft_o G} P(G/N, k)$.
- If G is a finite group, then

$$P(G, k) = \sum_{H \leq G} \frac{\mu_G(H)}{|G : H|^k}.$$

μ is the Möbius function of the subgroup lattice of G :

$$\mu_G(H) = \begin{cases} 1 & \text{if } H = G \\ -\sum_{H < K \leq G} \mu_G(K) & \text{otherwise} \end{cases}$$

THE SERIES (S)

Let G be a finitely generated profinite group and let

$$\sum_{H \leq_o G} \frac{\mu_G(H)}{|G:H|^k} \quad (S)$$

THE SERIES (S)

Let G be a finitely generated profinite group and let

$$\sum_{H \leq_o G} \frac{\mu_G(H)}{|G:H|^k} \quad (S)$$

Let $\{N_i\}_{i \in \mathbb{N}}$ be a chain of open normal subgroups with $\bigcap_{i \in \mathbb{N}} N_i = 1$.
Since

$$P(G, k) = \lim_{i \rightarrow \infty} P(G/N_i, k) = \lim_{i \rightarrow \infty} \left(\sum_{N_i \leq H \leq G} \frac{\mu_G(H)}{|G:H|^k} \right)$$

the series (S), with the above insertion of parentheses and with k replaced by a complex variable s , is a candidate for the conjectured function.

QUESTION

Does the series

$$\sum_{H \leq_o G} \frac{\mu_G(H)}{|G:H|^s} \quad (S)$$

converge in some half plane?

Different choices of the subgroup basis $\{N_i\}_{i \in \mathbb{N}}$ lead to different groupings of the terms in (S), so we have also to know whether two different bases lead to the same function.

Note that if (S) is absolutely convergent then its sum is independent of the ordering of the summands. In this case the sum would be independent of the choice of the basis $\{N_i\}_{i \in \mathbb{N}}$.

CONJECTURE (MANN 2005)

Let G be a PFG group. Then the infinite series converges absolutely in some right half plane.

$$\sum_{H \leq_o G} \frac{\mu_G(H)}{|G:H|^s} \quad (S)$$

CONJECTURE (MANN 2005)

Let G be a PFG group. Then the infinite series $\sum_{H \leq_o G} \frac{\mu_G(H)}{|G:H|^s}$ (S) converges absolutely in some right half plane.

SOME DEFINITIONS

- $b_n(G)$ the number of $H \leq G$ with $|G : H| = n$ and $\mu_G(H) \neq 0$
- $b_n(G)$ grows polynomially if there exists α such that

$$b_n(G) \leq n^\alpha \quad \forall n \in \mathbb{N}$$

- $\mu_G(H)$ grows polynomially if there exists β such that

$$|\mu_G(H)| \leq |G : H|^\beta \quad \forall H \leq_o G$$

PROPOSITION

The series (S) converges absolutely in some half plane if and only if both $\mu_G(H)$ and $b_n(G)$ grow polynomially.

CONJECTURE (MANN 2005)

Let G be a PFG group. Then the infinite series $\sum_{H \leq_o G} \frac{\mu_G(H)}{|G:H|^s}$ (S)
converges absolutely in some right half plane.

PARTIAL RESULTS

The conjecture has been proved:

- for profinite completions of arithmetic groups satisfying the congruence subgroup property (Mann 2005)
- for finitely generated prosolvable groups (AL 2007)

SUMMARIZING

We are dealing with the conjecture that if G is PFG then

$$\sum_{H \leq_o G} \frac{\mu_G(H)}{|G : H|^s}$$

converges absolutely in some right half plane.

This is equivalent to conjecture that in a PFG group G we have **polynomial bounds**

- for the number $b_n(G)$ of subgroups of index n with non trivial Möbius function, in term of n ,
- for the absolute value of $\mu_G(H)$, in term of $|G : H|$.

To discuss our conjecture we need to recall an important result on the behavior of maximal subgroups of PFG groups.

We say that G has **polynomial maximal subgroup growth** (PMSG) if there exists a number c such that for all $n \in \mathbb{N}$, the number $m_n(G)$ of maximal subgroups of G of index n is at most n^c .

THEOREM (MANN - SHALEV 1996)

G is PFG if and only if G has PMSG.

PROPOSITION

- *If H is an open subgroup of G and $\mu_G(H) \neq 0$, then H is an intersection of maximal subgroups.*
- *$|\mu_G(H)|$ is bounded by the number of ways to express H as an intersection of maximal subgroups.*

PROPOSITION

- *If H is an open subgroup of G and $\mu_G(H) \neq 0$, then H is an intersection of maximal subgroups.*
- *$|\mu_G(H)|$ is bounded by the number of ways to express H as an intersection of maximal subgroups.*

$b_n(G)$ is bounded in term of the number of maximal subgroups of G of index dividing n and $\mu_G(H)$ can be bounded in term of the number of maximal subgroups of G containing H .

Unfortunately, even if we assume that G is PMSG, the bounds that we obtain for $b_n(G)$ and $\mu_G(H)$ are not of polynomial type.

The best result that can be proved using these properties of the Möbius function is

THEOREM (MANN 1996)

Let G be a PMSG group, say $m_n(G) \leq n^c$. Then

- The number of maximal intersections of G of index at most n is not more than $n^{(c+1)\log n}$.
- $\sum_{|G:H| \leq n} |\mu_G(H)| \leq n^{2+(c+1)\log n}$.

If we want to obtain stronger bounds we need a better description of the subgroups with non trivial Möbius function. If $\mu_G(H) \neq 0$, then not only H is an intersection of maximal subgroups, but also these maximal subgroups can be chosen with additional good properties.

DEFINITION

Two chief factors A and B of G are **G -equivalent** ($A \sim_G B$) if either $A \cong_G B$ or there exists an open normal subgroup K of G such that G/K is a primitive permutation group with two different normal subgroups N_1 and N_2 and $A \cong_G N_1$, $B \cong_G N_2$.

DEFINITION

Two chief factors A and B of G are **G -equivalent** ($A \sim_G B$) if either $A \cong_G B$ or there exists an open normal subgroup K of G such that G/K is a primitive permutation group with two different normal subgroups N_1 and N_2 and $A \cong_G N_1$, $B \cong_G N_2$.

Two abelian chief factors are G -equivalent if and only if they are G -isomorphic, but for nonabelian chief factors G -equivalence is strictly weaker than G -isomorphism.

DEFINITIONS

Let A be a chief factor of G :

$$I_G(A) := \{g \in G \mid g \text{ induces an inner automorphism in } A\}$$

$$R_G(A) := \bigcap \left\{ R \trianglelefteq G \mid R \leq I_G(A), \frac{I_G(A)}{R} \sim_G A, \frac{I_G(A)}{R} \not\leq \text{Frat} \left(\frac{G}{R} \right) \right\}$$

The quotient group $I_G(A)/R_G(A)$ is called the **A-crown** of G .

There is a construction that can help to have a better understanding of the crowns.

There is a construction that can help to have a better understanding of the crowns.

Let L be a finite monolithic primitive group and let A be its unique minimal normal subgroup. The **crown-based power** of L of size k is the subgroup L_k of L^k defined by

$$L_k = \{(l_1, \dots, l_k) \in L^k \mid l_1 \equiv \dots \equiv l_k \pmod{A}\}.$$

There is a construction that can help to have a better understanding of the crowns.

Let L be a finite monolithic primitive group and let A be its unique minimal normal subgroup. The **crown-based power** of L of size k is the subgroup L_k of L^k defined by

$$L_k = \{(l_1, \dots, l_k) \in L^k \mid l_1 \equiv \dots \equiv l_k \pmod{A}\}.$$

If $G = L_k$, then

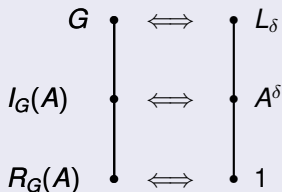
- $I_G(A) = A^k = \text{soc}(G)$,
- any minimal normal subgroup of G is G -equivalent to A ,
- $R_G(A) = 1$.

Let A be a chief factor of G . The **monolithic primitive group associated with A** is defined as

$$L = \begin{cases} A \times (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G/C_G(A) & \text{otherwise.} \end{cases}$$

If G is a finitely generated profinite group then

- in any chief series of G there are only finitely many non-Frattini chief factors G -equivalent to A ;
- the number δ of these chief factors is independent of the choice of the chief series;
- $R_G(A)$ is the largest open normal subgroup of G such that a chief series of $G/R_G(A)$ contains δ non-Frattini chief factors equivalent to A ;
- $G/R_G(A) \cong L_\delta$, $I_G(A)/R_G(A) \cong A^\delta$.



$R_G(A)$ is the intersection of the maximal subgroups M of G with the property that any minimal normal subgroup of $G/\text{Core}_G(M)$ is G -equivalent to A .

CHARACTERIZATION OF SUBGROUPS WITH NON TRIVIAL MÖBIUS FUNCTION

THEOREM

Assume that G is a finitely generated profinite group and let H be an open proper subgroup of G with $\mu_G(H) \neq 0$. There exists a finite family $\{Y_1, \dots, Y_t\}$ of open subgroups of G with the following properties:

- 1 $H = Y_1 \cap \dots \cap Y_t$
- 2 $|G : H| = |G : Y_1| \cdots |G : Y_t|$
- 3 for each $1 \leq j \leq t$, we have $\mu_G(Y_j) \neq 0$
- 4 for each $1 \leq j \leq t$, there exists a non-Frattini chief factor A_j of G with $R_G(A_j) \leq Y_j$ and $I_G(A_j) \not\leq Y_j$
- 5 if A_j is abelian, then Y_j is a maximal subgroup of G .

The proof is by induction on the order of $G/\text{Core}_G(H)$ and depends on two basic ingredients:

- **A consequence of the Complement Theorem of Crapo**

If N is normal subgroup of a finite group G , then

$$\mu_G(H) = \mu_G(HN) \sum_{Y \in \mathcal{S}} \mu_G(Y)$$

where $\mathcal{S} := \{Y \leq G \mid H \leq Y, YN = G, Y \cap N = H \cap N\}$.

- **A property of the crowns**

Let N be a minimal normal subgroup of a finite group G with $N \not\leq \text{Frat } G$. If $YN = G$ and $\mu_G(Y) \neq 0$, then $R_G(N) \leq Y$.

REDUCTION THEOREMS

THEOREM (AL 2009)

Assume that G is a PFG group and that there exists a constant c such that $b_n(G/R_G(A)) \leq n^c$ for each nonabelian chief factor A of G and each $n \in \mathbb{N}$. Then the sequence $\{b_n(G)\}_{n \in \mathbb{N}}$ has polynomial growth.

THEOREM (AL 2009)

Let G be a d -generated profinite group. Assume that there exist two constants c_1 and c_2 such that

$$b_n(G/R_G(A)) \leq n^{c_1} \quad \text{and} \quad |\mu_G(H)| \leq |G : H|^{c_2}$$

for each nonabelian chief factor A of G , each $R_G(A) \leq H \leq G$ and each $n \in \mathbb{N}$. Then, for each $H \leq G$,

$$|\mu_G(H)| < |G : H|^\alpha \quad \text{where} \quad \alpha = \max\{d, c_1 + c_2\}.$$

A FIRST APPLICATION: PSG GROUPS

Let G be a finitely generated profinite group. We denote by $a_n(G)$ the number of subgroups of G of index n .

We say that G has **polynomial subgroup growth** (PSG) if there exists a constant c such that $a_n(G) \leq n^c$ for each $n \in \mathbb{N}$.

A FIRST APPLICATION: PSG GROUPS

Let G be a finitely generated profinite group. We denote by $a_n(G)$ the number of subgroups of G of index n .
We say that G has **polynomial subgroup growth** (PSG) if there exists a constant c such that $a_n(G) \leq n^c$ for each $n \in \mathbb{N}$.

QUESTIONS

Is Mann's conjecture satisfied by PSG groups?

A FIRST APPLICATION: PSG GROUPS

Let G be a finitely generated profinite group. We denote by $a_n(G)$ the number of subgroups of G of index n .

We say that G has **polynomial subgroup growth** (PSG) if there exists a constant c such that $a_n(G) \leq n^c$ for each $n \in \mathbb{N}$.

QUESTIONS

Is Mann's conjecture satisfied by PSG groups?

If G has PSG, certainly the sequence $\{b_n(G)\}_{n \in \mathbb{N}}$ has polynomial growth, but it is not clear whether there exists a constant c with $|\mu_G(H)| \leq |G : H|^c$ for each open subgroup H of G .

A partial result in the PSG case follows from the following remark.

LEMMA (MANN)

Let G be a finite group and suppose that there exists a constant c such that $a_n(H) \leq n^c$ for each $n \in \mathbb{N}$ and each $H \leq G$. Then $|\mu_G(K)| \leq |G : K|^{c+2}$ for each subgroup K of G .

A partial result in the PSG case follows from the following remark.

LEMMA (MANN)

Let G be a finite group and suppose that there exists a constant c such that $a_n(H) \leq n^c$ for each $n \in \mathbb{N}$ and each $H \leq G$. Then $|\mu_G(K)| \leq |G : K|^{c+2}$ for each subgroup K of G .

PROOF

- $|\mu_G(K)|$ is bounded by the number of chains of subgroups connecting K to G .
- Let $K = K_t < K_{t-1} < \dots < K_0 = G$ be a chain, with indices $|K_{i-1} : K_i| = m_i$.
- For each i , the number of possibilities for K_i is at most m_i^c , so the number of possibilities for chains as above is at most $\prod_i m_i^c$.
- The number of possible ordered factorizations $|G : K| = m_1 \cdots m_t$ is at most $|G : K|^2$, so we get the bound $|\mu_G(K)| \leq |G : K|^{c+2}$.

A partial result in the PSG case follows from the following remark.

LEMMA (MANN)

Let G be a finite group and suppose that there exists a constant c such that $a_n(H) \leq n^c$ for each $n \in \mathbb{N}$ and each $H \leq G$. Then $|\mu_G(K)| \leq |G : K|^{c+2}$ for each subgroup K of G .

CONSEQUENCE

If G is **uniformly** a PSG group (i.e. there exists a number c such that $a_n(H) \leq n^c$ for each $n \in \mathbb{N}$ and each open subgroup H of G), then $|\mu_G(K)| \leq |G : K|^{c+2}$ for each open subgroup K of G .

The uniformly PSG groups are characterized as the groups of bounded upper rank. However using the reduction theorems the previous argument can be applied under the weaker assumption that only the nonabelian crowns have bounded rank.

DEFINITIONS

- The rank $r(X)$ of a finite group X is the smallest integer u with the property that all the subgroups of X can be generated by u elements.
- We will say that a finitely generated profinite group G **has nonabelian crowns of bounded rank** if there exists $u \in \mathbb{N}$ with the property that $r(I_G(A)/R_G(A)) \leq u$ for each nonabelian chief factor A of G .

THE MAIN RESULT

THEOREM (AL 2009)

Let G be a finitely generated profinite group. Assume that the nonabelian crowns of G have bounded rank. Then the series (S) converges absolutely in some right half plane.

THE MAIN RESULT

THEOREM (AL 2009)

Let G be a finitely generated profinite group. Assume that the nonabelian crowns of G have bounded rank. Then the series (S) converges absolutely in some right half plane.

If G has PSG, then G has nonabelian crowns of bounded rank.

COROLLARY

If a profinite group G has PSG (or more in general if G contains a closed prosolvable normal subgroup N such that G/N has PSG), then the series (S) converges absolutely in some right half plane.

REMARKS ON THE MAIN THEOREM AND ITS PROOF

If G has nonabelian crowns of bounded rank, then there exists n such that G is **Alt(n)-free** (i.e. no finite continuous epimorphic image of G involves $\text{Alt}(n)$ as a section).

REMARKS ON THE MAIN THEOREM AND ITS PROOF

If G has nonabelian crowns of bounded rank, then there exists n such that G is **Alt(n)-free** (i.e. no finite continuous epimorphic image of G involves $\text{Alt}(n)$ as a section).

Borovik, Pyber and Shalev (1996) proved that if G is a finitely generated profinite group and there is a finite group which is not obtained as a quotient of an open subgroup of G , then G is PFG. Hence if a finitely generated profinite group G has nonabelian crowns of bounded rank, then G is PFG.

REMARKS ON THE MAIN THEOREM AND ITS PROOF

A REMARK BY MANN

There exists a constant $c = c(u, m)$, which depends only on u and m , such that if X is $\text{Alt}(m)$ -free and $a_{n,u}(X)$ is the number of subgroups of index n of X that can be generated by u -elements, then $a_{n,u}(X) \leq n^c$.

REMARKS ON THE MAIN THEOREM AND ITS PROOF

A REMARK BY MANN

There exists a constant $c = c(u, m)$, which depends only on u and m , such that if X is $\text{Alt}(m)$ -free and $a_{n,u}(X)$ is the number of subgroups of index n of X that can be generated by u -elements, then $a_{n,u}(X) \leq n^c$.

Assume that $r(G/R_G(A)) \leq u$ for each nonabelian chief factor A of G .

- There exists m such that G is $\text{Alt}(m)$ -free.
- If $R_G(A) \leq K$, then $K/R_G(A)$ is $\text{Alt}(m)$ -free and all its subgroups are u -generated, so $a_n(K/R_G(A)) = a_{n,u}(K/R_G(A)) \leq n^c$.
- We deduce $b_n(G/R_G(A)) \leq n^c$ and $|\mu_G(H)| \leq |G : H|^{c+2}$ for each $R_G(A) \leq H \leq G$.
- We conclude by applying the reduction theorems.

There are other important families of finitely generated profinite groups with non abelian crowns of bounded rank.

A profinite group G is said to be **adelic** if G is isomorphic to a closed subgroup of

$$\mathrm{SL}(m, \hat{\mathbb{Z}}) \cong \prod_p \mathrm{SL}(m, \mathbb{Z}_p)$$

for some $m \geq 2$.

PROPOSITION

Every finitely generated adelic group has nonabelian crowns of bounded rank.

COROLLARY

If G is a finitely generated adelic profinite group, then the series (S) converges absolutely in some right half plane.

HOW CAN WE GET FURTHER RESULTS?

JAIKIN - PYBER

A finitely generated profinite group G is PFG if and only if there exists a constant c such that for any monolithic group L with a nonabelian socle A , the size of a crown-based power of L which occurs as a quotient of G is at most $I(A)^c$, where $I(A)$ is the minimal degree of a faithful transitive representation of A .

As a consequence Mann's conjecture can be reduced to the following:

CONJECTURE

For any constant c , there exist d_1 and d_2 such that: if L is a monolithic group with nonabelian socle A and $G = L_t$ with $t \leq I(A)^c$, then $|\mu_G(H)| \leq |G : H|^{d_1}$ for each core-free subgroup H and the number of core-free subgroups of index n with non trivial Möbius function is at most n^{d_2} .

A family N of natural numbers satisfies the **gcd** condition if there exists $\gamma \in \mathbb{N}$ such that for every finite subfamily F of N

$$\prod_{x \in F} \prod_{y \in F} \gcd(x, y) \leq \left(\prod_{x \in F} x \right)^\gamma.$$

THE PROFINITE PSG THEOREM

Let G be a profinite group. Then G has PSG if and only if G has closed normal subgroups $S \leq G_1$ such that S is prosoluble of finite rank, G/G_1 is finite, and G_1/S is a quasi-semisimple group of bounded type such that $\mathcal{N}(G_1/S)$ satisfies the gcd condition.

A profinite group Q is said to be quasi-semisimple of bounded type if Q is perfect and $Q/Z(Q) \cong \prod_i T_i$ where (T_i) is a sequence of finite simple groups of Lie type of bounded rank, each occurring with bounded multiplicity. Moreover $\mathcal{N}(Q)$ denotes the numerical sequence $(|T_i|)$. 